IN THE CLAIMS:

~~CLAIMS~~

There is claimed:

1. (Currently amended) A list signature method comprising ~~at least~~:

an organizing phase ~~(10) consisting~~including, for a reliable authority ~~(1)~~, ~~of~~ defining parameters for implementing an anonymous electronic signature, including a private key and a corresponding public key~~,~~;

a phase of registering ~~(20, 20')~~ persons in a list of members authorized to generate an electronic signature specific to the members of the list, during which each person ~~(2)~~ to be registered, calculates ~~(24)~~ a private key ~~(xi)~~ by means of parameters provided by the reliable authority and by parameters randomly selected by the person to be registered, and the reliable authority delivers ~~(25')~~ to each person to be registered, a certificate ~~([Ai, Ei])~~ of membership of the list~~,~~;

a phase of defining a sequence including for the reliable authority, generating a serial number to be used in a signing phase;

a signing phase ~~(30)~~ during which a member of the list generates ~~(35)~~ and issues ~~(36)~~ a signature specific to the members of the list, this signature being built so as to contain proof that the member of the list having issued the signature, has a certificate ~~([Ai, Ei])~~ of membership of the list, and a signature element which is common to all the signatures issued by a same member of the list with a same serial number and which contains proof that the serial number was used for generating the signature; ~~and~~

a phase of verifying ~~(40)~~ the issued signature, comprising steps ~~(41, 42) for~~ of applying a predefined algorithm in order to show proof that the signature was issued by a person having a certificate of membership of the list, and verifying using said signature element that the serial number was used for generating the signature;

~~characterized in that it further comprises:~~

~~a phase of defining a sequence consisting for the reliable authority (1), of generating a serial number (m) to be used in the signature phase (30), a signature (Siglist) generated during the signature phase comprising a signature element (T4) which is common to all the signatures issued by a same member of the list with a same serial number and which contains proof that the serial number (m) was used for generating the signature, the verifying phase (40) further comprising a phase for~~

~~verifying (43) the proof that the serial number (m) was used for generating the signature;~~

a phase of revoking a member of the list in order to remove a member from the list, during which the reliable authority ~~(1)~~ removes the member to be removed ~~withdrawn~~ from the list and updates the parameters for implementing the anonymous electronic signature, in order to take into account the removal of the member from the list; and

a phase of updating certificates ~~([Ai, ei])~~ of the members of the list in order to take into account changes in the composition of the list.

2. (Currently amended) (amended) The method according to claim 1, wherein the organizing phase ~~(10)~~ comprises the definition of a common parameter ~~(u)~~ depending on the composition of the list, the phase for registering ~~(20, 20')~~ a person in the list comprising the definition of a parameter ~~(ui)~~ specific to the person to be registered which is calculated according to the parameter ~~(u)~~ depending on the composition of the list and which is integrated into the certificate ~~([Ai, ei, ui])~~ handed out to the person, the registering phase ~~(20, 20')~~ comprising a step of updating the common parameter ~~(u)~~ depending on the composition of the list, the phase of revoking a member of the list comprising a step of changing the common parameter ~~(u)~~ depending on the composition of the list, in order to take into account the removal of the member from the list, and the phase of updating certificates of the members of the list including a step for updating the parameter ~~(ui)~~ specific to each member of the list in order to take into account changes in the composition of the list.

3. (Currently amended) The method according to claim 1 or 2, wherein a signature specific to a member of the list and having the certificate ~~[Ai, Ei]~~ comprises parameters T_1, T_2, T_3, such that:

$T_1 = A_i b^{\omega} \pmod{n}$,
$T_2 = g^{\omega} \pmod{n}$,
$T_3 = g^{e_i} h^{\omega} \pmod{n}$,

ω being a number randomly selected during the signing phase ~~(30)~~ and b, g, h and n being general parameters for implementing the group signature, such that parameters b, g and h cannot be inferred from each other by integer power raising modulo n functions, so that the number A_i, and therefore the identity of the member

of the list having the certificate $[A_i, e_i]$ cannot be inferred from a signature issued by the member.

4. (Currently amended) The method according to ~~any of the claims~~ claim 1 ~~to~~ ~~3~~, wherein the number ~~(m)~~ of the series used for generating a list signature is calculated as a function of a date of the beginning of the series.

5. (Original) The method according to claim 4, wherein the function for calculating the number of a series is of the form:

$F(d) = (H(d))^2 \pmod n$

wherein H is a collision-resistant hash function, d is the date of the beginning of the series, and n is a general parameter for implementing the group signature.

6. (Currently amended) The method according to ~~any of the claims~~ claim 1 ~~to~~ ~~5~~, wherein a signature issued by a member of the list contains a parameter which is calculated according to the serial number and the private key of the signatory member.

7. The method according to claim 6, wherein the parameter T_4 of a signature issued by a member of the list and depending on the serial number m and on the private key x_i of the signatory member is obtained by the following formula:

$T_4 = m^{x_i} \pmod n$

n being a general parameter for implementing the group signature, and the signature comprises proof that the parameter T4 was calculated with the private key xi of the member of the list who issued the signature.

8. (amended) An electronic voting method comprising:

~~a phase of organizing (50) elections, during which an organizing authority proceeds with generating parameters required for~~ an organizing phase of a poll including, for a reliable authority, defining parameters for implementing an anonymous electronic signature for being used to sign a ballot, said parameter including a private key and a corresponding public key; and ~~assigns~~ of assigning keys to scrutineers, allowing them to decrypt and verify ballots poll~~;~~;

a phase ~~for assigning a right of signature to each of the voters,~~ of registering voters in a list of voters authorized to generate an electronic signature specific to the members of the list, during which each voter to be registered calculates a private key by means of parameters provided by the reliable authority and by parameters randomly selected by the voter to be registered, and the reliable authority delivers to each voter to be registered, a certificate of membership of the list of voter;

a phase of defining a sequence for the elections including, for the reliable authority, generating a serial number to be used in a voting phase;

a voting phase ~~(60)~~ during which the voters of the list of voters sign a ballot by issuing a signature specific to the members of the list of voters, this signature being built so as to contain a proof that the member of the list of voters having issued the signature, has a certificate of membership of the list, and a signature element which is common to all the signatures issued by a same member of the list with a same serial number and which contains proof that the serial number was used for generating the signature; and

a counting phase ~~(70)~~ during which the scrutineers verify the ballots and calculate the result of the poll according to the contents of the decrypted and valid ballots, the verification of a ballot comprising steps of applying a predefined algorithm in order to show proof that the signature was issued by a person having a certificate of membership of the list of voters, and verifying using said signature element that the serial number was used for generating the signature, ~~characterized in that it implements a list signature method according to any of claims 1 to 7, for signing the ballots, each voter being registered as a member of a list, and a serial number (m) being generated for the poll,~~ in order to detect whether a same voter has issued several ballots for the poll or not;

a phase of revoking a member of the list of voters in order to remove a member from the list, during which the reliable authority removes the member to be removed from the list of voters and updates the parameters for implementing the anonymous electronic signature, in order to take into account the removal of the member from the list; and

a phase of updating certificates of the members of the list of voters in order to take into account changes in the composition of the list.

9. (Currently amended) The voting method according to claim 8, wherein the organizing phase ~~(50)~~ comprises the handing out to each scrutineer of a public key and a private key, the ballots ~~(v_i)~~ are encrypted ~~(62)~~ by means of a public key ~~(Y)~~ obtained by the product of the respective public keys (yi) of all the scrutineers, and the corresponding decryption private key ~~(X)~~ is obtained by calculating the sum of the respective private keys ~~(x_i)~~ of all the scrutineers

10. (Currently amended) The voting method according to claim 9, wherein encryption ~~(62)~~ of the ballot is carried out by means of a probabilistic encryption algorithm.

11. (Currently amended) The voting method according to ~~any of claims~~ claim ~~8 to 10~~, wherein the ballots issued by the votes are stored in a public database ~~(4)~~, in that the result of the verification and counting of each ballot is stored in the database in association with the ballot, and in that the private key ~~(X)~~ for decrypting the ballots is published.

12. (New) A server for organizing a list signature comprising means for:

generating parameters for implementing an anonymous electronic signature, specific to members of a list, said parameters including a private key and a corresponding public key;

transmitting each person to be registered in said list parameters to be used for calculating a private key by means of parameters randomly selected by the person to be registered, and a certificate of membership of the list;

generating a serial number to be used by the members registered in said list for generating an anonymous signature specific to the members of the list, this signature being built so as to contain a proof that the member of the list having issued the signature, has a certificate of membership of the list, and a signature element which is common to all the signatures issued by a same member of the list with a same serial number and which contains proof that the serial number was used for generating the signature;

removing a member of the list to be revoked, and updating the parameters for implementing the anonymous electronic signature, in order to take into account the removal of the revoked member from the list; and

updating the certificates of the members of the list each time the composition of the list is changed.

13. (New) A server for organizing an electronic vote comprising means for:

generating during a poll organization phase parameters for implementing an anonymous electronic signature for being used to sign a ballot, said parameter including a private key and a corresponding public key;

generating keys to be assigned to scrutineers, allowing them to decrypt and verify signatures of ballots issued by voters for the poll, said signature being specific to members of a list of voters;

transmitting to each person to be registered in the list of voters parameters to be used for calculating a private key by means of parameters randomly selected by the person to be registered, and a certificate of membership of the list;

generating a serial number specific to the poll, to be used by the members registered in said list of voters for generating an anonymous signature of a ballot specific to the members of the list of voters, this signature of a ballot being built so as to contain a proof that the member of the list of voters having issued the signature, has a certificate of membership of the list of voters, and a signature element which is common to all the signatures issued by a same member of the list of voters with a same serial number and which contains proof that the serial number was used for generating the signature;

removing a member of the list of voters to be revoked, and updating the parameters for implementing the anonymous electronic signature, in order to take into account the removal of the revoked member from the list of voters; and

updating the certificates of the members of the list of voters each time the composition of the list for the poll is changed.

14. (New) A terminal for generating a list signature comprising means for:

receiving from a reliable authority parameters to be used for calculating a private key;

calculating a private key by means of the received parameters and parameters randomly selected;

receiving from the reliable authority a certificate of membership of the list;

receiving a serial number to be used for generating an anonymous signature specific to the members of the list;

generating an anonymous signature specific to the members of the list, this signature being built so as to contain a proof that the member of the list having issued the signature, has a certificate of membership of the list, and a signature element which is common to all the signatures issued by a same member of the list with a same serial number and which contains proof that the serial number was used for generating the signature;

verifying a signature issued by a member of said list by applying a predefined algorithm in order to show proof that the signature was issued by a person having a certificate of membership of the list, and by verifying using said signature element that the serial number was used for generating the signature; and

receiving a new certificate of membership of the list each time the composition of the list is changed.

15. (New) A terminal for issuing an electronic signature of a ballot during an electronic vote, comprising means for:

receiving from a reliable authority parameters to be used for calculating a private key;

calculating a private key by means of the received parameters and parameters randomly selected;

receiving from the reliable authority a certificate of membership of a list of voters;

receiving a serial number to be used for generating an anonymous signature of a ballot for said poll, said signature being specific to the members of the list of voters;

generating an anonymous signature specific to the members of the list of voters, this signature being built so as to contain a proof that the member of the list of voters having issued the signature, has a certificate of membership of the list of voters, and a signature element which is common to all the signatures issued by a same member of the list of voters with a same serial number and which contains proof that the serial number was used for generating the signature;

verifying a signature issued by a member of said list of voters by applying a predefined algorithm in order to show proof that the signature was issued by a

person having a certificate of membership of the list of voters, and by verifying using said signature element that the serial number was used for generating the signature; and

receiving a new certificate of membership of the list of voters each time the composition of the list of voters is changed.